IN THE CLAIMS:
Please revise the claims, as follows:

1-2. (Canceled)

3. (Previously presented) The method according to claim 39, wherein said object comprises a smart card.

4. (Original) The method according to claim 3, wherein said smart card incorporates a chip.

5-7. (Canceled)

8. (Previously presented) The method according to claim 39, further comprising:

reading, by a reader, the sample in an imprecise manner, meaning that sequential readings are not exactly the same as an initial reading of said sample, but collecting, at a time of preparation of the object more information about said sample than will be contained by decoding any of said coded version of that information,

wherein said object carries a chip and a recording of a digital representation of the full information initially collected of the sample from the reader used at the time the object is prepared.

9. (Original) The method according to claim 8, further comprising:

sending a result of the reader to a processor, which associates with the reading of the sample said number;

sending said number to a second processor containing a secure hash function, details of which are made public, and a secret part of said key signature, said key signature comprising a public key signature, wherein said second processor computes a coded version of the hash of said number appended with a predetermined, optional data; and

outputting said coded version to said chip.

10. (Original) The method according to claim 9, wherein upon introducing the object into a second reader, a different reading of said sample occurs such that the first reader reads the sample to deliver *R(S)* and the second reader reads the sample to deliver *R0(S0)*, said method further comprising:

determining by a comparator whether the readings by said first and second readers are less than or equal to a predetermined threshold to accept the object, at least temporarily, as authentic.

11. (Previously presented) The method according to claim 10, further comprising:

reading said coded version by said chip and verifying said coded version against said number by using a public part of the public key signature; and

if said number and said coded version read by said chip are compatible, accepting the object as authentic.

12. (Original) The method according to claim 8, further comprising:

delivering by said reader an actual reading *R(S)* and delivering by a second reader an original reading as *R0(S0)*;

processing said readings by first and second processors to deliver *N(R(S)* and *N(R0(S0))*, respectively; and

determining by a comparator whether outputs from said first and second processors have a value no more than a predetermined threshold, to temporarily accept the object as authentic.

13. (Original) The method according to claim 12, further comprising:

reading the coded version in said chip and verifying said coded version against said number by using a public portion of a public key signature; and

if the information in said number and that read in said chip are compatible, accepting said object as authentic.

14. (Previously presented) The method according to claim 39, further comprising:

sensing a degeneration of said sample.

15. (Original) The method according to claim 14, wherein said sensing includes comparing a difference between an actual reading vector and an original reading vector against a threshold;

forwarding a result of the reader to a processor, which associates with the reading of said sample a transformed vector *K(N0(R0(S0)))*, where *K* is a transformation matrix; and

forwarding the transformed vector to a second processor including a secure hash function, details of which are made public, and a secret part of a public key signature scheme.

16. (Previously presented) The method according to claim 15, wherein said object includes a chip, and wherein said second processor computes a coded version of the hash function of the

transformed vector appended with predetermined external data, to provide a coded number, said coded number being put on said chip,

wherein upon introducing the object to a second reader, a predetermined different reading of the sample is performed.

17. (Original) The method according to claim 16, wherein an actual reading made by a first reader is transformed into a transformed vector *KN*, and wherein an original transformed vector *KN0* is delivered by a second reader, and

wherein the transformed vector, *KN* is compared against the original transformed vector *KN0* by a comparator such that if the two transformed vectors have a value within a predetermined closeness, the object is temporarily accepted as authentic.

18. (Previously presented) The method according to claim 17, further comprising:

reading by said chip the coded version and verifying said coded version against the transformed vector using a public part of the public key signature; and

accepting the object as authentic if the transformed vector and the coded version read in said chip are compatible.

19. (Previously presented) The method according to claim 39, wherein said object being authenticated comprises a piece of paper.

20. (Previously presented) The method according to claim 39, wherein a sequence of data associated with said sample, said sample, and certificates associated with said sample and said data are precomputed.

21. (Previously presented) The method according to claim 20, wherein new data and its certificate are computed dynamically.

22. (Previously presented) The method according to claim 39, wherein said key signature includes using private key cryptography.

23. (Previously presented) The method according to claim 39, wherein said specific reader captures information out of the sample by one of a scanning and globally.

24. (Previously presented) The method according to claim 39, wherein said sample includes at least one of an exposed face of a mineral sample and an exposed face of a glass sample, selectively covered by a carbon film and affixed to said object.

25. (Previously presented) The method according to claim 39, wherein said coded version of said number includes at least one of optional data appended to said number and a hash of said number with said optional data.

26. (Previously presented) The method according to claim 39, wherein data linked to the sample of material is selectively changeable during at least one reading subsequent to an initial reading of said sample at said time of production.

27. (Previously presented) The method according to claim 39, wherein said sample of material is selectively changeable over time.

28. (Previously presented) The method according to claim 39, wherein said data is selectively changeable when said sample is changed.

29. (Original) The method according to claim 20, wherein said data is selectively changeable when said sample is changed.

30. (Previously presented) The method according to claim 39, wherein new data associated with said sample and a certificate of said sample are computed dynamically.

31. (Previously presented) The method according to claim 39, wherein at a time of creation of said object, said coded version of said number is stored in memory for later comparison when said object is presented for authentication.

32. (Previously presented) The method according to claim 39, wherein a plurality of coded versions of numbers are recorded into said object.

33-36. (Canceled)

37. (Previously presented) The method of claim 39, wherein said forming at least one coded version of said number further comprises using additional information for said forming said coded version, wherein said additional information comprises the date of issue of said object.

38. (Previously presented) The method of claim 39, wherein said forming at least one coded version of said number further comprises using additional information for said forming said coded version, wherein said additional information comprises the functionality of an application of said object.

39. (Currently amended) A method of guaranteeing authenticity of an object that includes or has attached thereto at least one of a chip with a recording support and another recording support, said method comprising:

attaching to said object a first sample of material obtainable by at least one of a chemical process and a physical process having a characteristic that samples generated by said process are random and non-reproducible, said first sample being associated with a first number obtained by reading said first sample using a first reader of a specific sort;

recording, on at least one of said recording supports, at said time of production, in an exactly readable way, ~~an exact value~~ a representation of said first number so that said first number can be checked against a later reading made with any reader of said specific sort at each time of verification of said object, thereby providing a first verification that verifies that a sample being read at said verification of said object is indeed said first sample; and

forming, at said time of production, at least one encrypted version of said first number, at least one of said encrypted versions of said first number being also recorded in an exactly readable way on said object at said time of production, said at least one encrypted version of said first number being obtained by a method from public key cryptography, said recording of said at least one encrypted version thereby providing a second verification that verifies at said verification that said encrypted version of said first number was generated by an authorized party,

wherein information concerning said public key cryptography method is available so that said second verification can be made by anyone of an intended public and said first number is recorded as an unencrypted number.

40. (Previously presented) The method of claim 39, wherein said first number is encrypted in combination with further information, said further information and all encrypted versions of said first number being also recorded in an exactly readable way on said object at said time of production.

41. (Previously presented) The method of claim 39, further comprising:

forming at least one second encrypted version of said first number by a private key cryptography encryption scheme; and

recording said at least one second encrypted version in an exactly readable manner on said object.

42-44. (Canceled)

45. (Previously presented) The method of claim 39, wherein said first number is converted into and recorded in a base 3 number format.

46-49. (Canceled)

50. (Currently amended) ~~The method of claim 49~~ A method of guaranteeing authenticity of an object, said object including at least one of a chip having a first recording support and a second recording support, said method comprising:

providing a sample of material obtainable only by at least one of chemical and physical processes such that a measurable characteristic of said sample is random and not reproducible and affixing said sample to said object;

using a reader to take a measurement of said characteristic of said sample, said measurement becoming a number reproducibly associated to said sample; and

to allow for sample-reader combinations such that the number associated to said sample is not exactly reproducible at a time of verification, recording said number as an unencrypted number read by said reader on said object on at least one of said first recording support and said second recording support,

wherein said process provides a sample that degenerates over time in a manner that can be measured and said number is recorded on said object along with a time stamp when said reading occurs, and

wherein a subsequent reading of said sample is used to determine whether a negative-degeneration has occurred for said sample, said negative-degeneration indicating that a tampering has occurred to said sample.

51-53. (Canceled)